IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appellants:	Slawomir Ilnicki et al.	Examiner: Christopher A. Revak
Serial No.:	09/592,322	Group Art Unit: 2131
Filed:	June 13, 2000	Docket No.: 10992668-1
Title:	Secure Data Transfer Method and System	

REPLY APPEAL BRIEF UNDER 37 C.F.R. § 41.41

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants request that this appeal be maintained by filing of this Reply Brief in accordance with 37 C.F.R. § 41.41.

This Reply Appeal Brief is filed in response to the non-final Office Action mailed November 3, 2005 stating new grounds of rejection in response to Appellant's Appeal Brief filed on January 5, 2005.

AUTHORIZATION TO DEBIT ACCOUNT

It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's deposit account no. 08-2025.

REAL PARTY IN INTEREST

The real party-in-interest is the assignee, Hewlett-Packard Company, a Delaware corporation, having its principal place of business in Palo Alto, California.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals or interferences known to appellant, the appellant's legal representative, or assignee that will directly affect or be directly affected by or have a bearing on the Appeal Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1 – 22 and 24 – 26 stand finally rejected. No claims have been allowed. The final rejection of claims 1 – 22 and 24 – 26 is appealed.

STATUS OF AMENDMENTS

All claim amendments have been entered. Claims 1 – 22 and 24 – 26 are pending in the application. Claim 23 has been canceled.

SUMMARY OF CLAIMED SUBJECT MATTER

The following provides a concise explanation of the subject matter defined in each of the claims involved in the appeal, referring to the specification by page and line number and to the drawings by reference characters, as required by 37 C.F.R. § 41.37(c)(1)(v). Each element of the claims is identified by a corresponding reference to the specification and drawings where applicable. Note that the citation to passages in the specification and drawings for each claim element does not imply that the limitations from the specification and drawings should be read into the corresponding claim element or that these are the sole sources in the specification supporting the claim features.

Claim 1

A method for securely transferring data between an agent and an application server through a non-secure node (Fig. 3, block 314; Fig. 5; Page 8, lines 10+) comprising:

(a) establishing a session key between the agent and the application server by utilizing a public key of the application server (Fig. 3, block 304; Fig. 4; Page 9, lines 21-25); wherein the public key of the application server is embedded in the agent to enable the agent to derive the session key (Fig. 4, #408; Page 10, lines 7-31); and

(b) establishing an end-to-end secure connection between the agent and the application server by using the session key and by establishing a communication link between the application server and the non -secure node by using a relay module (Fig. 3, block 308; Fig. 6; Fig. 8; corresponding description to figures).

Claim 11

The method of securely transferring data between an application server and an agent of the application server through a non-secure environment having a web-server and the agent (Fig. 3, block 314; Fig. 5; Page 8, lines 10+), the method comprising:

a) a user accessing the web-server to download the agent therefrom (Fig. 4, #400; Page 10, lines 1-5); wherein the agent includes a public key of the application server (Page 10, lines 1-13);

b) the agent deriving a shared session key with the application server by using the public key of the application server, the shared session key for use in encrypting and decrypting data to be transferred between the agent and the application server (Fig. 3, block 304; Fig. 4, #408; Page 10, lines 14-31);

c) the application server establishing a connection to the web-server (Fig. 3, block 308; Fig. 8); and

d) the agent contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server (Fig. 3, block 314; Fig. 7; Fig. 8; corresponding description to figures).

Claim 15

A secure data transfer system for connecting a non-secure node to an application server behind a firewall (Fig. 5, #500; Page 8, lines 10-15) comprising:

a) a web-server (Fig. 5, # 540) in the non-secure node (Fig. 5, # 530; Page 8, lines 22-24);

b) a relay (Fig. 5, # 560) in the non-secure node that is dynamically instantiated by the application server (Fig. 5, # 524), the relay being configured by the application server to have a first port (Fig. 5, # 561) for listening for a connection from the application server (Fig. 6; Fig. 8; Page 8, line 25 – page 9, line 8);

wherein the application server connects to the relay on the first port and reads data from the first port (Fig. 6; Fig. 8; Page 9, lines 1-8).

Claim 17

A secure data transfer system for establishing an end-to-end secure connection between an agent and an application server behind a firewall through a non-secure node (Fig. 5, # 500; Page 8, lines 10-15) comprising:

a) a web-server (Fig. 5, # 540) residing in the non-secure node (Fig. 5, # 530), the web-server having the agent that includes a public key of the application server (Fig. 5, # 524; Page 8, lines 10-24);

b) a browser (Fig. 5, # 510) in communication with the web-server for downloading the agent from the web-server (Page 8, lines 19-21);

c) a secure transfer module (Fig. 5, # 548) residing in the non-secure node (Fig. 5, # 530; Page 8, lines 25-30); and

d) an application server (Fig. 5, # 524) in a secure zone (Fig. 5, # 520) for initiating a connection to the web-server via the secure transfer module (Fig. 3; Page 8, lines 25-30; Fig. 3).

Claim 22

A method, comprising:

embedding in code of an agent a public key of an application server that is behind a firewall (Fig. 4, #400; Page 10, lines 1-6; Fig. 5);

downloading the code of the agent and the public key into a browser (Fig. 4, #400; Page 10, lines 1-6; Fig. 5);

verifying the agent to authenticate the public key of the application server (Fig. 4, # 404; Page 10 line 7 – page 11, line 8);

establishing a communication link between the application server and a relay module that is in a non-secure environment and between the browser and the relay module (Fig. 3, block 308; Fig. 5; Fig. 6; Page 9, lines 25-28); and

securely transferring data from the browser through the relay module to the application server without requiring a trusted intermediate party (Fig. 3, block 314; Fig. 5; Fig. 8; Page 9, lines 28-29).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

I. Claims Rejection - 35 USC § 102(e)

Claims 11, 14, 17, 19, and 21 are rejected under 35 USC § 102(e) as being anticipated by USPN 6,757,825 (hereinafter MacKenzie).

II. Claims Rejection (Claims 6-8) – 35 USC § 103(a)

Claims 1-10, 12, 13, 15, 16, 18, 20, 22, and 24-26 are rejected under 35 USC §103(a) as being unpatentable over MacKenzie.

ARGUMENT

The rejection of claims 1 – 22 and 24 – 26 is improper, and Applicants respectfully request reversal of the rejections.

The claims do not stand or fall together. Instead, Applicants present separate arguments for various independent and dependent claims. Each of these arguments is separately argued below and presented with separate headings and sub-heading as required by 37 C.F.R. § 41.37(c)(1)(vii).

Overview of MacKenzie

As discussed in the background of MacKenzie, "[a]uthentication over a network is an important part of security for systems that allow remote clients to access network servers" (1: 12-14). One technique for network authentication is called "password-only authentication" wherein a client provides a legitimate password to access a server (2: 24-27). "The problem with these known password-only authentication protocols is that they have not been proven secure" (2: 61-62). MacKenzie solves this problem by providing a secure password-only authentication protocol in which a server generates public key and secret key pairs and transmits the public key to a client (3: 4-12). The client receives the public key and determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). If the public key is not within the testable superset, then the client rejects authentication. Otherwise, protocol continues (3: 12-23).

Lack of Specificity in Office Action

Independent claims 1, 11, 15, 17, and 22 recite numerous different elements. In rejecting these claims, however, the Office Action merely cites a large section of MacKenzie (namely, column 3 lines 5-17 and column 8, lines 12-27). The Office Action, however, never specifies which portions of MacKenzie correspond to which elements in the independent claims. In other words, the Office Action never argues or specifies which elements of MacKenzie's system correspond with the words or elements in the claims. Instead, the Office Action copies the claims and cites the noted section of MacKenzie at the end of the copied claim. Applicants believe that such specificity is not stated because MacKenzie does not teach or suggest an apparatus, system or method that has elements

as recited in the claims. Additionally, Applicants admit that it is difficult to rebut the Office Action since the action makes broad generalizations to reject the claims, instead of specifying which portions of MacKenzie's teachings correspond to which elements in the claims.[1]

I. Claims Rejection - 35 USC § 102(e)

Claims 11, 14, 17, 19, and 21 are rejected under 35 USC § 102(e) as being anticipated by USPN 6,757,825 (hereinafter MacKenzie). Appellants respectfully traverse. Each of the independent claims (11 and 17) is separately argued below with a separate sub-heading.

Claim 11

Claim 11 recites numerous limitations that are not taught or suggested in MacKenzie; examples are discussed below. For convenience, claim 11 is reproduced (emphasis added):

> The method of securely transferring data between an application server and an agent of the application server through a non-secure environment having a web-server and the agent, the method comprising:
>
> a) **a user accessing the web -server to download the agent therefrom; wherein the agent includes a public key of the application server;**
>
> b) **the agent deriving a shared session key with the application server by using the public key of the application server,** the shared session key for use in encrypting and decrypting data to be transferred between the agent and the application server;
>
> c) the application server establishing a connection to the web-server; and
>
> d) **the agent** contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server.

[1] In rejecting independent claims 11 and 17, for example, the Office Action quotes the claim then merely cites MacKenzie at col. 3, lines 5-17 and col. 8, lines 12-27 for teaching all of the various claimed elements.

On numerous occasions, claim 11 recites recitations pertaining to an agent. MacKenzie does not teach the limitations of claim 11 regarding the agent. In fact, MacKenzie is not directed to agents at all. The word "agent" or discussions about "agents" does not even occur in MacKenzie.

According to MPEP § 2111.01, the words of a claim must be given their "plain meaning." Webopedia is an online dictionary for computer and internet technology definitions. According to Webopedia (see www.webopedia.com), an agent is defined as: "A program that performs some information gathering or processing task in the background. Typically, an agent is given a very small and well-defined task." Appellants submit that MacKenzie does not teach or suggest "agents" per the plain meaning of this term.

Appellants acknowledge that claims must be given their broadest interpretation during patent examination. However, this interpretation must be a "**reasonable interpretation consistent with the specification**" (see MPEP 2111: emphasis added). Appellants specification repeatedly uses the term "agent" in a manner consistent with the plain meaning of this term. Appellants respectfully ask the Board of Appeals to read Appellants' Background of the Invention for a discussion of exemplary agents.

As one example, claim 11 recites "a user accessing the web-server to download the agent therefrom." The Office Action cites MacKenzie at column 3, lines 5-17 and column 8, lines 12-27 for teaching this recitation. These sections of MacKenzie have nothing whatsoever to do with downloading agents. By contrast, the section at column 3 teaches secure password-only authentication protocol in which a server transmits a public key to a client, and the client determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). Nowhere does this section teach or suggest that a user downloads an "agent" from a web-server. Further, the section at column 8 teaches a client and server that generate session and secret keys to establish secure communication between the client and server. Nowhere does this section teach or suggest that a user downloads an "agent" from a web-server.

Applicants strongly argue that a "client" is **not** an "agent." These two terms have entirely different meanings to one of ordinary skill in the art. According to Webopedia (see www.webopedia.com), a client is defined as:

> A client is an application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

Appellants specification repeatedly uses the term "client" in a manner consistent with the plain meaning of this term.

For at least these reasons, claim 11 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As another example, claim 1 recites that the agent includes a public key of the application server. The Office Action cites MacKenzie at col. 3, lines 5-17 and col. 8, lines 12-27. Appellants respectfully assert that the Office Action is citing unrelated sections of MacKenzie. Again, column 3 of MacKenzie teaches secure password-only authentication protocol in which a server transmits a public key to a client, and the client determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). Nowhere does this section teach or suggest that an agent itself includes a public key of an application server. Column 8 of MacKenzie teaches a client and server that generate session and secret keys to establish secure communication between the client and server. Nowhere does this section teach or suggest that an agent itself includes a public key of an application server.

For at least these reasons, claim 11 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet another example, claim 11 recites that **the agent derives** a shared session key with the application sever by using the public key of the application server. This recitation is not taught or suggested in MacKenzie. The Office Action cites columns 3 and 8 of MacKenzie. Column 3 of MacKenzie teaches secure password-only authentication protocol in which a server transmits a public key to a client, and the client

determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). Nowhere does this section teach or suggest that an "agent" itself derives a shared session key. An agent and client have different meanings to one of ordinary skill in the art. MacKenzie does not even mention agents or using agents. Column 8 of MacKenzie teaches a client and server that generate session and secret keys to establish secure communication between the client and server. Nowhere does this section teach or suggest that an "agent" itself derives a shared session key. Again, MacKenzie does not even mention agents or using agents.

For at least these reasons, claim 11 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet another example, claim 11 recites that the agent contacts the web server using a first protocol. The Office Action cites columns 3 and 8 of MacKenzie. These sections of MacKenzie do not even contemplate an agent, let alone "the agent contacting the web server ...."

For at least these reasons, claim 11 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet another example, element d) of claim 11 recites recitations regarding both an application server and a web-server. Column 3 of MacKenzie does not even mention two different kinds of servers, let alone an application server and a web-server. By contrast, column 3 only mentions one kind of server: a network server. Likewise, column 8 only mentions the same network server. Notice that claim 11 recites two different kinds of servers: application server and web-server.

For at least these reasons, claim 11 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

Claim 17

Claim 17 recites numerous limitations that are not taught or suggested in MacKenzie; examples are discussed below. For convenience, claim 17 is reproduced (emphasis added):

A secure data transfer system for establishing an end-to-end secure connection between an agent and an application server behind a firewall through a non-secure node comprising:

a) a web-server residing in the non-secure node, the web-server having the agent that includes a public key of the application server;

b) a browser in communication with the web-server for downloading the agent from the web-server;

c) a secure transfer module residing in the non-secure node; and

d) an application server in a secure zone for initiating a connection to the web-server via the secure transfer module.

On numerous occasions, claim 17 recites recitations pertaining to an agent. MacKenzie does not teach the limitations of claim 17 regarding the agent. In fact, MacKenzie is not directed to agents at all. The word "agent" or discussions about "agents" does not even occur in MacKenzie.

For at least these reasons, claim 17 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As another example, claim 17 recites establishing an end-to-end secure connection between "an agent and an application server." The Office Action cites MacKenzie at column 3, lines 5-17 and column 8, lines 12-27 for teaching this recitation. Applicants respectfully disagree. Column 3 of MacKenzie teaches secure password-only authentication protocol in which a server transmits a public key to a client, and the client determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). Nowhere does this section teach or suggest establishing a secure connection between an agent an application server. Column 8 of MacKenzie teaches a client and server that generate session and secret keys to establish secure communication between the client and server. Nowhere does this section teach or suggest establishing a secure connection between an agent and an application server. Applicants respectfully ask the Board of Appeals to construe the word "agent" per the plain meaning of this term as understood in the art.

For at least these reasons, claim 17 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As another example, claim 17 recites: "the web-server having the agent that includes a public key of the application server." In other words, the agent itself includes a public key of the application server. The Office Action cites MacKenzie at column 3, lines 5-17 and column 8, lines 12-27 for teaching this recitation. Applicants respectfully disagree. Column 3 of MacKenzie teaches secure password-only authentication protocol in which a server transmits a public key to a client, and the client determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). Nowhere does this section teach or suggest that a web-server has an agent that includes a public key of the application server. Column 8 of MacKenzie teaches a client and server that generate session and secret keys to establish secure communication between the client and server. Nowhere does this section teach or suggest that a web-server has an agent that includes a public key of the application server.

For at least these reasons, claim 17 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet another example, claim 17 recites recitations regarding both an application server and a web-server. Column 3 of MacKenzie does not even mention two different kinds of servers, let alone an application server and a web-server. By contrast, column 3 only mentions one kind of server: a network server. Likewise, column 8 only mentions the same network server. Notice that claim 17 recites two different kinds of servers: application server and web-server.

For at least these reasons, claim 17 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet another example, claim 17 recites "a secure transfer module residing in the non-secure node." The Office Action has not identified any element in MacKenzie that corresponds to a "secure transfer module residing in a non-secure node." The Office Action cites MacKenzie at column 3, lines 5-17 and column 8, lines 12-27 for teaching this recitation. Applicants respectfully disagree since these sections have nothing to do with a secure transfer module that resides in a non-secure node.

For at least these reasons, claim 17 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

II. Claims Rejection (Claims 6-8) – 35 USC § 103(a)

Claims 1-10, 12, 13, 15, 16, 18, 20, 22, and 24-26 are rejected under 35 USC §103(a) as being unpatentable over MacKenzie. Appellants respectfully traverse. Each of the independent claims (1, 15, and 22) is separately argued below with a separate sub-heading.

Overview of Law on Section 103

To establish a prima facie case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art cited must teach or suggest all the claim limitations. *See* M.P.E.P. § 2143. Applicants assert that the rejection does not satisfy these criteria.

I. No Suggestion/Motivation to Modify MacKenzie

For at least the following reasons, no suggestion or motivation exists to modify MacKenzie.

The Office Action argues that it would be obvious to modify MacKenzie to include a router to establish a communication link between the application server and a non-secure node using a relay module. Applicants respectfully disagree. MacKenzie expressly solves the problem that password-only authentication protocols in the past have not been secure (2: 61-62). MacKenzie solves this problem by providing a secure password-only authentication protocol in which a server generates public key and secret key pairs and transmits the public key to a client (3: 4-12). Nowhere does MacKenzie teach or suggest how its embodiments would use a router to establish a communication link between an application server and a non-secure node.

The Examiner must provide *objective evidence*, rather than subjective belief and unknown authority, of the requisite motivation or suggestion to combine or modify the cited references. *In re Lee*, 61 U.S.P.Q.2d. 1430 (Fed. Cir. 2002). Obviousness cannot be established by combining the teachings of the prior art to produce the claimed invention

absent some teaching or suggestion supporting the combination. *ACS Hospital Systems, Inc. v. Montefiore Hospital*, 732 F.2d 1572, 1577, 221 U.S.P.Q. 929, 933 (Fed. Cir. 1984). Such teaching or suggestion does not exist.

Further, to establish a *prima facie* case, the Examiner must not only show that the combination includes *all* of the claimed elements, but also a convincing line of reason as to why one of ordinary skill in the art would have found the claimed invention to have been obvious in light of the teachings of the references. *Ex parte Clapp*, 227 U.S.P.Q. 972 (B.P.A.I. 1985).

For at least these reasons, Applicant respectfully asks the Board of Appeals to withdraw the rejection since a *prima facie* case of obvious has not been established.

II. No Reasonable Expectation of Success

No reasonable expectation of success has been established for modifying MacKenzie. MacKenzie expressly solves the problem that password-only authentication protocols in the past have not been secure (2: 61-62). MacKenzie solves this problem by providing a secure password-only authentication protocol in which a server generates public key and secret key pairs and transmits the public key to a client (3: 4-12). If MacKenzie incorporates a router in non-secure node, then MacKenzie would no longer provide the noted security for its password-only authentication protocol.

In view of these deficiencies, the Office Action has failed to establish a reasonable expectation of success with a modification of MacKenzie. Therefore, the *prima facie* case of obviousness has not been established.

III. All Elements Not Taught or Suggested

All of the elements of the claims are not taught or suggested in MacKenzie. In other words, evening assuming *arguendo* that MacKenzie is successfully combinable (which it is not), the alleged modification does not teach or suggest all the elements in the claims. Examples for various independent are provided below.

Claim 1

Claim 1 recites numerous limitations that are not taught or suggested in MacKenzie; examples are discussed below. For convenience, claim 1 is reproduced (emphasis added):

> A method for securely transferring data between **an agent** and an application server through a non-secure node comprising:
>
> (a) establishing a session key between **the agent** and the application server by utilizing a public key of the application server; **wherein the public key of the application server is embedded in the agent to enable the agent to derive the session key**; and
>
> (b) establishing an end-to-end secure connection between **the agent** and the application server by using the session key and by establishing a communication link between the application server and the non-secure node by using a relay module.

On numerous occasions, claim 1 recites recitations pertaining to an **agent**. MacKenzie does not teach the limitations of claim 1 regarding the agent. In fact, MacKenzie is not directed to agents at all. The word "agent" or discussions about "agents" does not even occur in MacKenzie.

Appellants respectfully ask the Board of Appeals to construe the word "agent" in a manner consistent with the specification and the plain meaning of this term. Appellants respectfully ask the Board of Appeals to read Appellants' Background of the Invention for a discussion of exemplary agents.

As further examples, claim 1 recites:

1) securely transferring data between **an agent** and an application server,
2) establishing a session key between **the agent** and the application server,
3) wherein the public key of the application server is embedded in **the agent**,
4) establishing an end-to-end secure connection between **the agent** and the application server.

Nowhere does MacKenzie teach or suggest using an agent as recited in claim 1. For at least these reasons, Appellants respectfully request withdrawal of the rejection.

As an additional example, claim 1 recites that "the public key of the application server is embedded in the agent to enable the agent to derive the session key." This recitation is not taught in MacKenzie. The Office Action cites MacKenzie at col. 3, lines 5-17 and col. 8, lines 12-27. Appellants respectfully assert that the Office Action is citing unrelated sections of MacKenzie. Column 3 of MacKenzie teaches secure password-only authentication protocol in which a server transmits a public key to a client, and the client determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). Nowhere does this section teach or suggest that the public key of the application server is **embedded in the agent** to enable **the agent to derive** the session key. Column 8 of MacKenzie teaches a client and server that generate session and secret keys to establish secure communication between the client and server. Nowhere does this section teach or suggest that the public key of the application server is **embedded in the agent** to enable **the agent to derive** the session key.

For at least these reasons, claim 1 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet another example, claim 1 recites establishing a secure connection between an agent and an application server. The Office Action cites MacKenzie at col. 3, lines 5-17 and col. 8, lines 12-27. Appellants respectfully assert that these sections of MacKenzie have nothing to do with establishing a connection between an agent and an application server.

For at least these reasons, claim 1 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

Claim 15

Claim 15 recites numerous limitations that are not taught or suggested in MacKenzie; examples are discussed below. For convenience, claim 15 is reproduced (emphasis added):

A secure data transfer system for connecting a non-secure node to an application server behind a firewall comprising:

a) a web-server in the non-secure node;

b) a relay in the non-secure node that is dynamically instantiated by the application server, **the relay being configured by the application server to have a first port for listening for a connection from the application server;**

wherein the application server connects to the relay on the first port and reads data from the first port.

Claim 15 recites recitations regarding both an application server and a web-server. Column 3 of MacKenzie does not even mention two different kinds of servers, let alone an application server and a web-server. By contrast, column 3 only mentions one kind of server: a network server. Likewise, column 8 only mentions the same network server. Notice that claim 15 recites two different kinds of servers: application server and web-server.

For at least these reasons, claim 15 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As another example, claim 15 recites that the relay is "configured by the application server." This recitation is not taught in MacKenzie. The Office Action has not cited a location in MacKenzie for teaching or suggesting this recitation. Instead, the Office Action cites MacKenzie at column 3, lines 5-17 and column 8, lines 12-27 for teaching this recitation. These sections of MacKenzie have nothing whatsoever to do with configuring relays. By contrast, the section at column 3 teaches secure password-only authentication protocol in which a server transmits a public key to a client, and the client determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). Nowhere does this section teach or suggest that a relay is configured by an application server. Further, the section at column 8 teaches a client and server that generate session and secret keys to establish secure communication between the client and server. Nowhere does this section teach or suggest that a relay is configured by an application server.

For at least these reasons, claim 15 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet another example, claim 15 recites that the relay is configured by the application server to have "a first port for listening for a connection from the application server." This limitation is not taught or suggested in MacKenzie. The Office Action has not cited a location in MacKenzie for teaching or suggesting this recitation. Instead, the Office Action cites MacKenzie at column 3, lines 5-17 and column 8, lines 12-27 for teaching this recitation. These sections of MacKenzie have nothing whatsoever to do with listening for a connection from an application server. By contrast, the section at column 3 teaches secure password-only authentication protocol in which a server transmits a public key to a client, and the client determines if this key is an element of "a so-called testable superset" of the set of all public keys (3: 12-14). Nowhere does this section teach or suggest listening for a connection from the application server. Further, the section at column 8 teaches a client and server that generate session and secret keys to establish secure communication between the client and server. Nowhere does this section teach or suggest listening for a connection from the application server.

For at least these reasons, claim 15 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

Claim 22

Claim 22 recites numerous limitations that are not taught or suggested in MacKenzie; examples are discussed below. For convenience, claim 22 is reproduced (emphasis added):

> A method, comprising:
>
> embedding in code of **an agent** a public key of an application server that is behind a firewall;
>
> downloading the code of **the agent** and the public key into a browser;
>
> verifying **the agent** to authenticate the public key of the application server;

establishing a communication link between the application server and a relay module that is in a non-secure environment and between the browser and the relay module; and

securely transferring data from the browser through the relay module to the application server without requiring a trusted intermediate party.

On numerous occasions, claim 22 recites recitations pertaining to an agent. MacKenzie does not teach the limitations of claim 22 regarding the agent. In fact, MacKenzie is not directed to agents at all. The word "agent" or discussions about "agents" does not even occur in MacKenzie.

Appellants respectfully ask the Board of Appeals to construe the word "agent" in a manner consistent with the specification and the plain meaning of this term. Appellants respectfully ask the Board of Appeals to read Appellants' Background of the Invention for a discussion of exemplary agents.

For at least these reasons, claim 22 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet numerous other examples, Appellants note at least the following occurrences of the term "agent" in claim 22:

1) embedding in code of **an agent** a public key of an application server,
2) downloading the code of **the agent**, and
3) verifying **the agent**.

MacKenzie does not teach or suggest any of these limitations. The Office Action has not cited a location in MacKenzie for teaching or suggesting this recitation. Instead, the Office Action cites MacKenzie at column 3, lines 5-17 and column 8, lines 12-27 for teaching this recitation. These sections of MacKenzie have nothing whatsoever to do with the elements as recited in claim 22.

For at least these reasons, claim 22 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

As yet another example, claim 22 recites "verifying the agent." The Office Action does not even address this recitation. In other words, the Final Office Action does not provide a section in MacKenzie that teaches or suggests this recitation. Appellants have reviewed MacKenzie and find no such teaching or suggestion.

For at least these reasons, claim 22 is allowable over MacKenzie. The dependent claims are allowable for at least these reasons.

CONCLUSION

In view of the above, Appellants respectfully request the Board of Appeals to reverse the Examiner's rejection of all pending claims.

Any inquiry regarding this Appeal should be directed to Philip S. Lyren at Telephone No. (281) 514-8236, Facsimile No. (281) 514-8332. In addition, all correspondence should continue to be directed to the following address:

Hewlett-Packard Company
Intellectual Property Administration
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,

Philip S. Lyren
Reg. No. 40,709
Ph: 281-514-8236

CERTIFICATE UNDER 37 C.F.R. 1.8

The undersigned hereby certifies that this paper or papers, as described herein, is being transmitted to the United States Patent and Trademark Office facsimile number 571-273-8300 on this 27th day of January, 2006.

By: Carrie McKerley
Name: Carrie McKerley

VIII. Claims Appendix

1. A method for securely transferring data between an agent and an application server through a non-secure node comprising:

(a) establishing a session key between the agent and the application server by utilizing a public key of the application server; wherein the public key of the application server is embedded in the agent to enable the agent to detive the session key; and

(b) establishing an end-to-end secure connection between the agent and the application server by using the session key and by establishing a communication link between the application server and the non -secure node by using a relay module.

2. The method of claim 1 wherein establishing a communication link between the application server and the non-secure node by using a relay module comprises:

dynamically instantiating, by the application server, the relay module having a first port for communicating with the application server and a second port for communicating with the agent, the relay module listening on a first predetermined port number on the first port and a second predetermined port number on the second port; and

the application server connecting to the first port of the relay module to establish a connection therewith.

3. The method of claim 2 wherein establishing a communication link between the application server and the agent through a relay module further comprises:

pushing data encrypted by the established session key from the agent to the application server over the end-to-end secure connection.

4. The method of claim 2 wherein establishing a communication link between the application server and the agent through a relay module further comprises:

pulling data encrypted by the session key from the application server over the end-to-end secure connection to the agent.

5. The method of claim 1 wherein establishing a session key between the agent and the application server by utilizing a public key of the application server further comprises:

establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween.

6. The method of claim 5 wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween comprises:

encrypting the shared secret key with the public key of the application server to generate an encrypted shared key;

sending the encrypted shared secret key to the application server; and

decrpyting the shared secret key with the private key of the application server.

7. The method of claim 5 wherein establishing a shared secret key between the application server and the agent utilizes a key transfer protocol.

8. The method of claim 7 wherein the key transfer protocol is the Rivest, Shamir, Adleman (RSA) public key algorithm.

9. The method of claim 5 wherein establishing a shared secret key between the application server and the agent for encrypting and decrypting data sent therebetween utilizes a key agreement protocol.

10. The method of claim 9 wherein the key agreement protocol is the Diffie-Hellman (DH) public key algorithm.

11. The method of securely transferring data between an application server and an agent of the application server through a non-secure environment having a web-server and the agent, the method comprising:

a) a user accessing the web-server to download the agent therefrom; wherein the agent includes a public key of the application server;

b) the agent deriving a shared session key with the application server by using the public key of the application server, the shared session key for use in encrypting and decrypting data to be transferred between the agent and the application server;

c) the application server establishing a connection to the web-server; and

d) the agent contacting the web server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server.

12. The method of claim 11 wherein the application server establishing a connection to the web-server further comprises

c1) the application server dynamically instantiating a relay module by sending a URL associated with the relay module to the web-server, the URL specifying a first predetermined port for communication between the web-server and the relay module;

c2) the application server connecting to the relay module on a first predetermined port; and

c3) the application server reading data from the relay module through the connection on the first predetermined port.

13. The method of claim 12 wherein the agent contacting the web-server by using a first protocol to send data encrypted by the session key to the application server over the connection between the web-server and the application server further comprises

d1) the agent encrypting the session key with the public key of the application server;

d2) the agent collecting data;

d3) the agent encrypting the collected data with the session key;

d4) sending the encrypted session key and encrypted measured data to the application server by using a forwarding module that connects to a second predetermined port of the relay module.

14. The method of claim 11 wherein the first protocol is one of HTTP and HTTP/SSL.

15. A secure data transfer system for connecting a non-secure node to an application server behind a firewall comprising:

a) a web-server in the non-secure node;

b) a relay in the non-secure node that is dynamically instantiated by the application server, the relay being configured by the application server to have a first port for listening for a connection from the application server;

wherein the application server connects to the relay on the first port and reads data from the first port.

16. The secure data transfer system of claim 15 wherein the relay does not initiate the connection with the application server but waits for the application server to establish the connection.

17. A secure data transfer system for establishing an end-to-end secure connection between an agent and an application server behind a firewall through a non-secure node comprising:

a) a web-server residing in the non-secure node, the web-server having the agent that includes a public key of the application server;

b) a browser in communication with the web-server for downloading the agent from the web-server;

c) a secure transfer module residing in the non-secure node; and

d) an application server in a secure zone for initiating a connection to the web-server via the secure transfer module.

18. The secure data transfer system of claim 17 wherein the secure transfer module further comprises:

c1) a relay module for listening to a first port and a second port;

c2) an instantiation module for executing the relay module in response to a command from the application server;

c3) a forwarding module for transferring data from the agent to the relay module in response to a command from the agent; and

wherein the relay module listens to the first port for a connection by the application server and listens to the second port for a connection by the forwarding module.

19. The secure data transfer system of claim 16 wherein the non -secure node is a web-server node.

20. The method of claim 1 further comprising transferring data between the agent and the relay module via an unsecure communication link.

21. The method of claim 11 comprising transferring data between the agent and the web-server via an unsecure communication link.

22. A method, comprising:

embedding in code of an agent a public key of an application server that is behind a firewall;

downloading the code of the agent and the public key into a browser;

verifying the agent to authenticate the public key of the application server;

establishing a communication link between the application server and a relay module that is in a non-secure environment and between the browser and the relay module; and

securely transferring data from the browser through the relay module to the application server without requiring a trusted intermediate party.

23. (canceled)

24. The method of claim 22 further comprising collecting data with the agent.

25. The method of claim 24 wherein collecting data with the agent further comprises measuring time required to load data into the browser.

26. The method of claim 22 wherein the communication link between the browser and the relay module is an unsecure communication link.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.